REMARKS

This is a full and timely response to the outstanding non-final Office Action mailed January 26, 2007. Claims 1-49 remain pending in the present application. Reconsideration and allowance of the application and pending claims are respectfully requested.

1. Response to Rejections of Claims under 35 U.S.C. §102

Claims 1-7, 10-13, 16-20, 22-24, 26-38, 41-43, and 46-49 have been rejected under 35 U.S.C. §102(b) as being anticipated by *Bennett* ("Experimental Quantum Cryptography," September 1991, pp. 1-28 obtained from http://cs.uccs.edu/~cs691/crypto/BBBSS92.pdf). Applicants respectfully traverse this rejection.

It is axiomatic that "[a]nticipation requires the disclosure in a single prior art reference of each element of the claim under consideration." *W. L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1554, 220 USPQ 303, 313 (Fed. Cir. 1983). Therefore, every claimed feature of the claimed subject matter must be represented in the applied reference to constitute a proper rejection under 35 U.S.C. §102(b). In the present case, not every feature of the claimed subject matter is represented in the *Bennett* reference. Applicants discuss the *Bennett* reference and Applicants' claims in the following.

a. Claim 1

As provided in independent claim 1, Applicants claim:

> A method of establishing a shared secret random cryptographic key between a sender and a recipient using a quantum communications channel, the method comprising:
>
> ***generating a plurality of random quantum states of a quantum entity, each random state being defied by a randomly selected one of a first plurality of bases in Hilbert space, the first plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space;***
>
> transmitting the plurality of random quantum states of the quantum entity via the quantum channel to the recipient;
>
> ***measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a second plurality of bases in Hilbert space, the second plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space;***

> transmitting to the recipient composition information describing a subset of the plurality of random quantum states;
>
> analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states;
>
> establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar;
>
> deriving, a first binary string and a second binary string, correlated to the first binary string, respectively from the transmitted and received plurality of quantum states not in the subset; and
>
> carrying out a reconciliation of the second binary string to the first binary string by using error correction techniques to establish the shared secret random cryptographic key from the first and second binary strings.

(Emphasis added).

Applicants respectfully submit that independent claim 1 is allowable for at least the reason that *Bennett* does not disclose, teach, or suggest at least "generating a plurality of random quantum states of a quantum entity, each random state being defied by a randomly selected one of a first plurality of bases in Hilbert space, the first plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space" and "measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a second plurality of bases in Hilbert space, the second plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space," as recited and emphasized above in claim 1.

Rather, *Bennett* describes that a sender (Alice) sends a random sequence of four kinds of polarized photons to a receiver (Bob). *See* page 4. As such, Alice sends one of only four kinds of photons to Bob. Accordingly, *Bennett* fails to teach or suggest at least "generating a plurality of random quantum states of a quantum entity, each random state being defied by a randomly selected one of a first plurality of bases in Hilbert space, the first plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space," as recited in claim 1. (Emphasis added).

Further, *Bennett* describes that the receiver (Bob) chooses to randomly measure a received photon's rectilinear or circular polarization. Thus, the receiver has one of two options from which to choose. *See* page 4. Accordingly, *Bennett* fails to teach or suggest at least "measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a second plurality of bases in Hilbert space, <u>the second plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space</u>," as recited in claim 1. (Emphasis added).

Hence, claim 1 is not anticipated by *Bennett*, and the rejection should be withdrawn.

b. <u>Claims 2-7, 10-13, 16-20, and 22-24</u>

Because independent claim 1 is allowable over the cited art of record, dependent claims 2-7, 10-13, 16-20, and 22-24 (which depend from independent claim 1) are allowable as a matter of law for at least the reason that dependent claims 2-7, 10-13, 16-20, and 22-24 contain all the features of independent claim 1. For at least this reason, the rejections of claims 2-7, 10-13, 16-20, and 22-24 should be withdrawn. Additionally, claims 2-7, 10-13, 16-20, and 22-24 recite additional features not taught or suggested by the cited art.

Withdrawal of the rejections is respectfully requested.

c. <u>Claim 26</u>

As provided in independent claim 26, Applicants claim:

> A method of a sender establishing a secret random cryptographic key shared with a recipient using a quantum communications channel, the method comprising:
>
> ***generating a plurality of random quantum states of a quantum entity, each random state being defined by a randomly selected one of a first plurality of bases in Hilbert space, the first plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space;***
>
> transmitting the plurality of random quantum states of the quantum entity via the quantum channel to the recipient;
>
> transmitting to the recipient composition information describing a subset of the plurality of random quantum states;
>
> deriving a first binary string from the transmitted plurality of quantum states not in the subset; and

> using error correction techniques to establish the shared secret random cryptographic key from the first binary string.

(Emphasis added).

Applicants respectfully submit that independent claim 26 is allowable for at least the reason that *Bennett* does not disclose, teach, or suggest at least "generating a plurality of random quantum states of a quantum entity, each random state being defined by a randomly selected one of a first plurality of bases in Hilbert space, the first plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space," as recited and emphasized above in claim 26.

Rather, *Bennett* describes that a sender (Alice) sends a random sequence of four kinds of polarized photons to a receiver (Bob). *See* page 4. As such, Alice sends one of only four kinds of photons to Bob. Accordingly, *Bennett* fails to teach or suggest at least "generating a plurality of random quantum states of a quantum entity, each random state being defined by a randomly selected one of a first plurality of bases in Hilbert space, the first plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space," as recited in claim 26. (Emphasis added).

Hence, claim 26 is not anticipated by *Bennett*, and the rejection should be withdrawn.

d. Claims 27-34

Because independent claim 26 is allowable over the cited art of record, dependent claims 27-34 (which depend from independent claim 26) are allowable as a matter of law for at least the reason that dependent claims 27-34 contain all the features of independent claim 26. For at least this reason, the rejections of claims 27-34 should be withdrawn. Additionally, claims 27-34 recite additional features not taught or suggested by the cited art.

e. Claim 35

As provided in independent claim 35, Applicants claim:

> A method of a recipient establishing a secret random cryptographic key shared with a sender using a quantum communications channel, the method comprising:

receiving a plurality of random quantum states of a quantum entity via the quantum channel from the sender;

measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a recipient's plurality of bases in Hilbert space, the second plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space;

receiving from the sender composition information describing a subset of the plurality of random quantum states;

analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states;

establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar;

deriving a recipient binary string from the received plurality of quantum states not in the subset; and

using error correction techniques to establish the shared secret random cryptographic key from the recipient binary string.

(Emphasis added).

Applicants respectfully submit that independent claim 35 is allowable for at least the reason that *Bennett* does not disclose, teach, or suggest at least "measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a recipient's plurality of bases in Hilbert space, the second plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space," as recited and emphasized above in claim 35.

Rather, *Bennett* describes that a sender (Alice) sends a random sequence of four kinds of polarized photons to a receiver (Bob). *See* page 4. Further, *Bennett* describes that the receiver (Bob) chooses to randomly measure a received photon's rectilinear or circular polarization. Thus, the receiver has one of two options from which to choose. *See* page 4. Accordingly, *Bennett* fails to teach or suggest at least "measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a recipient's plurality of bases in Hilbert space, <u>the second plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space</u>," as recited in claim 35. (Emphasis added).

Hence, claim 35 is not anticipated by *Bennett*, and the rejection should be withdrawn.

f. Claims 36-38, 41-43, and 46-49

Because independent claim 35 is allowable over the cited art of record, dependent claims 36-38, 41-43, and 46-49 (which depend from independent claim 35) are allowable as a matter of law for at least the reason that dependent claims contain all the features of independent claim 35. For at least this reason, the rejections of claims 36-38, 41-43, and 46-49 should be withdrawn. Additionally, claims 36-38, 41-43, and 46-49 recite additional features not taught or suggested by the cited art.

2. Response to Rejections of Claims under 35 U.S.C. §103

Claims 8, 9, 21, 25, 39, and 40 have been rejected under 35 U.S.C. §103(a) as purportedly being unpatentable over *Bennett* in view of *Black* ("Quantum Computing and Communication," pp. 1-52, obtained from http://hissa.nist.gov/~black/Papers/ quantumCom.pdf). Claims 14-15 and 44-45 have been rejected under 35 U.S.C. §103(a) as purportedly being unpatentable over *Bennett* in view of *Franson* (U.S. Patent No. 6,678,450). Claim 25 has been rejected under 35 U.S.C. §103(a) as purportedly being unpatentable over *Bennett* in view of *Franson* in further view of *Black*.

All of the claimed features of independent claims 1 and 35 are not taught and suggested by *Bennett*, as previously discussed. Further, the cited art of *Black* and *Franson* fails to cure the deficiencies of the *Bennett* reference in suggesting or teaching all of the claimed features in independent claims 1 and 35 and dependent claims 8-9, 14-15, 21, 25, 39-40, and 44-45 which depend there from. Therefore, a *prima facie* case establishing an obviousness rejection by the proposed combination of *Bennett* in view of *Black* and/or *Franson* has not been made. For at least this reason, the rejections of claims 8-9, 14-15, 21, 25, 39-40, and 44-45 should be withdrawn.

CONCLUSION

For at least the reasons set forth above, Applicants respectfully submit that all objections and/or rejections have been traversed, rendered moot, and/or accommodated, and that the pending claims are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned agent at (770) 933-9500.

Respectfully submitted,

Charles W. Griggers
Reg. No. 47,283